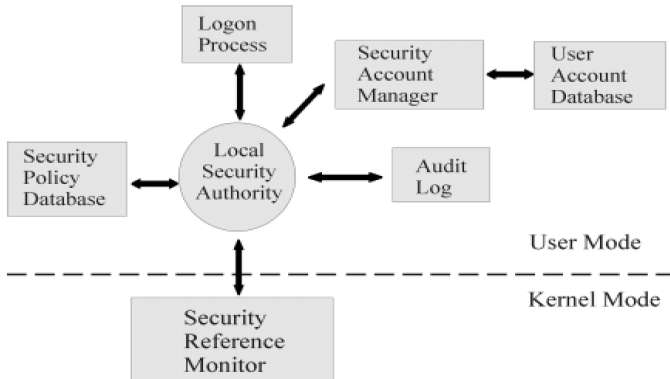
**Security Architecture of Windows**

**There are three components of Windows Security:**  
⎫ LSA (Local Security Authority)  
⎫ SAM (Security Account Manager)  
⎫ SRM (Security Reference Monitor)

[](http://article1000.com/wp-content/uploads/2017/08/Security-Architecture-of-Windows.png)

Security Architecture of Windows

**LSA (Local Security Authority)**

ϖ LSA is the Central Part of NT Security. It is also known as Security Subsystem. The Local Security Authority or LSA is a key component of the logon process in both Windows NT and Windows 2000. In Windows 2000, the LSA is  
responsible for validating users for both local and remote logons. The LSA also maintains the local security policy.  
ϖ During the local logon to a machine, a person enters his name and password to the logon dialog. This information  
is passed to the LSA, which then calls the appropriate authentication package. The password is sent in a nonreversible secret key format using a one-way hash function. The LSA then queries the SAM database for the User’s account information. If the key provided matches the one in the SAM, the SAM returns the users SID and the SIDs of any groups the user belongs to. The LSA then uses these SIDs to generate the security access token.

**SAM (Security Account Manager)**

ϖ The Security Accounts Manager is a database in the Windows operating system (OS) that contains user names and  
passwords. SAM is part of the registry and can be found on the hard disk.  
ϖ This service is responsible for making the connection to the SAM database (Contains available user-accounts and  
groups). The SAM database can either be placed in the local registry or in the Active Directory (If available). When  
the service has made the connection it announces to the system that the SAM-database is available, so other  
services can start accessing the SAM-database.  
ϖ In the SAM, each user account can be assigned a Windows password which is in encrypted form. If someone  
attempts to log on to the system and the user name and associated passwords match an entry in the SAM, a  
sequence of events takes place ultimately allowing that person access to the system. If the user name or  
passwords do not properly match any entry in the SAM, an error message is returned requesting that the  
information be entered again.  
ϖ When you make a New User Account with a Password, it gets stored in the SAM File.  
ϖ Windows Security Files are located at “C:\Windows\System32\Config\SAM”  
ϖ The moment operating system starts, the SAM file becomes inaccessible.

**SRM (Security Reference Monitor)**

ϖ The Security Reference Monitor is a security architecture component that is used to control user requests to  
access objects in the system. The SRM enforces the access validation and audit generation. Windows NT forbids  
the direct access to objects. Any access to an object must first be validated by the SRM. For example, if a user  
wants to access a specific file the SRM will be used to validate the request. The Security Reference Monitor  
enforces access validation and audit generation policy.  
ϖ The reference monitor verifies the nature of the request against a table of allowable access types for each process  
on the system. For example, Windows 3.x and 9x operating systems were not built with a reference monitor,  
whereas the Windows NT line, which also includes Windows 2000 and Windows XP, was designed with an entirely  
different architecture and does contain a reference monitor.